Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

КРИПТОГРАФІЯ

Комп’ютерний практикум №3

«Криптоаналіз афінної біграмної підстановки»

Варіант №2

Виконали:

студенти групи ФБ-93

Бурячок А.А

Данілін Д.Д.

Перевірила:

Селюх П.В.

Київ - 2021

Мета: набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки, опанування приймами роботи в модулярній арифметиці.

Завдання:

- уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
- реалізувати підпрограми із необхідними математичними операціями: обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
- за допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифротексту (2 варіант).
- перебрати можливі варіанти співставлення частих біграм мови і частих біграм шифротексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співпадіння знайти можливі кандидати на ключ (a, b) шляхом розв'язання системи.
- для кожного кандидата на ключ дешифрувати шифротекст. Якщо шифротекст не є змістовним текстом російської мовою, відкинути цього кандидата.
- повторювати дії 3-4 доти, доки дешифрований текст не бути змістовним.

Хід роботи:

Частина 1

Реалізуємо підпрограми, які будуть обчислювати обернений елемент за модулем, який використовує розширений метод Евкліда, розв'язувати лінійні рівняння. Результати роботи знаходяться у файлі main.cpp.

Частина 2

За допомогою програми, яку ми робили під час виконання комп’ютерного практикуму №1, знаходимо найчастіші біграми у зашифрованому тексті. Таблиця з усіма результатами наведена нижче.

Відкриптий текст	Шифрований текст
то: 0.017742	йа: 0.019766
ен: 0.013435	юа: 0.018152
но: 0.012735	чш: 0.016539
на: 0.011974	юд: 0.014522
ст: 0.011974	рщ: 0.012505

Частина 3

Перебираємо всі можливі перестановки довжиною 5 (120 шт). Для кожної такої перестановки знаходимо можливого кандидата на ключ (пара a, b) шляхом розв’язання системи лінійних порівнянь. Таблиця з усіма отриманими ключами наведена нижче, а також у файлі permutations.txt.

Отримані ключі афінної підстановки						
27, 211	110, 779	118, 295	120, 211	137, 469	170, 0	196, 267
223, 536	224, 584	230, 469	263, 620	290, 893	314, 41	342, 941
396, 60	400, 190	423, 953	538, 687	561, 489	565, 956	619, 317
647, 800	671, 365	698, 55	731, 713	737, 91	738, 264	765, 196
791, 55	824, 372	841, 589	843, 164	851, 645	934, 10	934, 248

Під час перебору кожної перестановки ми розв’язували 4 системи з двох лінійних порівнянь. Для деякої перестановки ми отримали, що ключ (27, 211) переводить всі найчастіші біграми відкритого тексту (російської мови) у всі біграми шифрованого тексту. Результати обчислень наведені нижче, а також у файлі keys.txt.

Перестановка $(\frac{1\,2\,3\,4\,5}{1\,4\,2\,5\,3})$					
ВТ	то	ен	но	на	ст
ШТ	йа	юд	юа	рщ	чш

Частина 4

Для кожного кандидата на ключ дешифруємо шифрований текст. Перевіряємо текст на змістовність за допомогою обчислення індексу відповідності. Серед усіх варіантів відкритого тексту, найбільш змістовним є той, який ми отримали шляхом розшифрування шифрованого тексту ключем a = 27, b = 211. При цьому значення індексу відповідності приймає значення 0.053, що є найближчим до істинного значення для російської мови. Додатково перевірили, що частоти літер “о”, “е”, “а” лежать у межах істинних значень для російської мови (відповідно [0.08, 0.12], [0.07, 0.1], [0.06, 0.1]). Результат відкритого тексту, який ми отримали, наведено у файлі text.txt.

Висновки: під час виконання комп’ютерного практикуму №3 ми ознайомилися із афінним шифром та однією з його варіацій - афінною біграмною підстановкою. Нами були розвинені навички в модулярній арифметиці та частотному криптоаналізі. Зрозуміли, як розв’язувати лінійні порівняння. Знайшли всіх кандидатів на ключ і обрали серед них єдиний - конкретний, за допомогою якого змогли розшифрувати зашифрований текст.